

Bâtiment 'Le Zénith'
Boulevard du Roi Albert II, 37
1030 Bruxelles

Plateforme Services Web ETNIC
-
Spécifications techniques

Produit :	**Plateforme Services Web ETNIC**
Type de document :	**Manuel d'utilisation**
Révision du document :	**1.0**
Date du document :	**22-04-2014**

Historique

Version	Description	Ecrit par	Date
1.0	Version initiale	Anne Noseda Xavier Martin	22-04-2014

Objectifs du document

Ce document est destiné aux partenaires désireux d'intégrer leurs applications à celles de la Fédération Wallonie-Bruxelles en utilisant la plateforme de Services Web mise à disposition par l'ETNIC.

La plateforme est d'abord présentée de manière conceptuelle et puis définie techniquement domaine par domaine.

Public cible

Ce document s'adresse principalement aux architectes, analystes et développeurs.

Contacts

Pour toute question ou demande d'assistance technique veuillez contacter le helpdesk de l'ETNIC.

Support général
Email : support@etnic.be
Tél : 02 / 800 10 10

Table des matières

1. PRESENTATION DE LA PLATEFORME SERVICES WEB DE L’ETNIC

1.1. Cadre

L'ETNIC expose des Services Web sur Internet à destination de ses partenaires informatiques désireux d’intégrer leurs applications avec les services de la Fédération Wallonie-Bruxelles.

L’ensemble des Services Web sont exposés à travers une plateforme technique répondant à diverses spécifications portant entre autre sur le protocole de communication et la sécurité.

1.2. Caracteristiques

La communication se fait de manière **asynchrone** à travers un canal sécurisé par **TLS**. Les Services Web dialoguent avec des messages **SOAP** sécurisés selon la spécification **WS-Security** et signés avec un certificat numérique. Selon le type de certificat utilisé, les spécifications **WSS-x509TokenProfile**, **WS-SecureConversation** et **WS-Trust** sont utilisées.

Les sections suivantes de ce document décrivent en profondeur les spécifications techniques à satisfaire pour pouvoir dialoguer avec la plateforme.

1.3. Acces

Actuellement seuls des services du domaine de l’enseignement sont exposés. Pour ceux-ci, quel que soit le service adressé, le point d’accès à la plateforme est unique.

Les URLs pour les différents environnements sont les suivantes :

- Test & Qualification : https://services-web.tq.etnic.be/ecole
- Production : https://services-web.etnic.be/ecole

Avant de pouvoir accéder à la plateforme, vous devez dans un premier temps créer un compte Cerbère auprès de l’ETNIC. Le certificat de votre carte d’identité électronique est nécessaire pour cet enregistrement et donc un lecteur de carte. Les URLs pour s’enregistrer dans les deux environnements sont les suivantes :

- Test & Qualification :
https://www.users-acceptance.cfwb.be/IDMProv/portal/cn/GuestContainerPage/SelfRegisterID?population=EDU&eid=true&aff=VDB2WndlbDNvLzl0dHVIQnpTbW4xVGgyZVh4SXhJNXQNCg

- Production :
https://www.users.cfwb.be/IDMProv/portal/cn/GuestContainerPage/SelfRegisterID?population=EDU&eid=true&aff=Wi92ZklvaVMvQVYrSk9TVURwWUo5Vjd2eCt6Q3lHaFkNCg

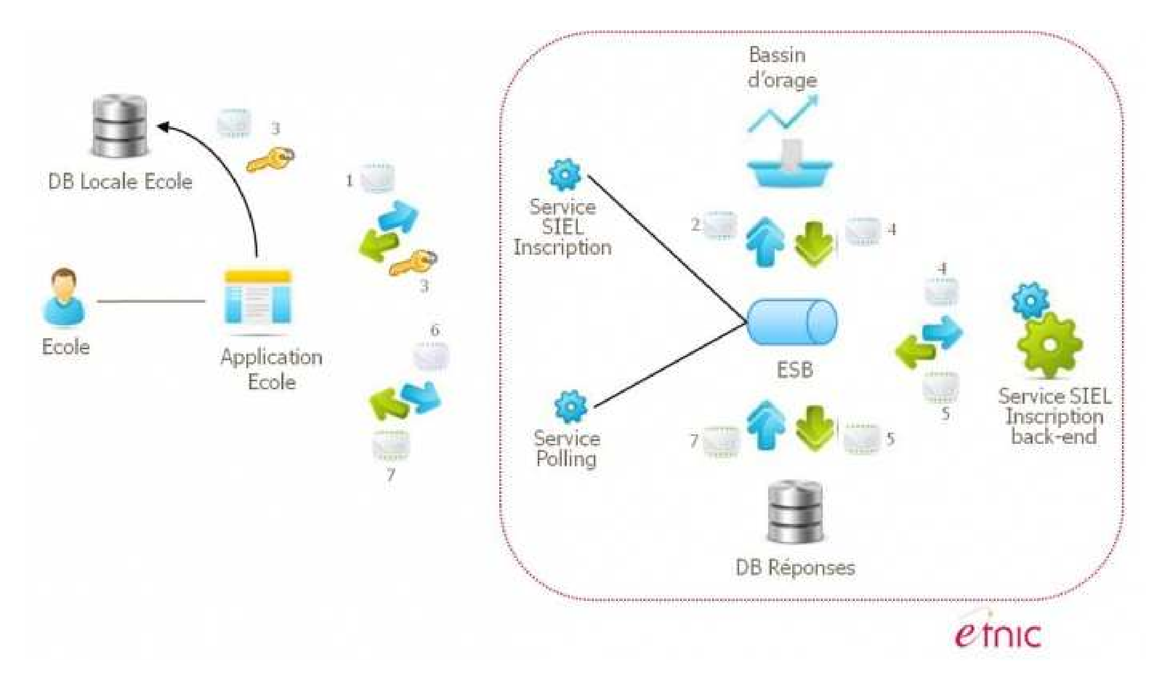
Vous devrez alors fournir le certificat que vous utiliserez pour vous connecter aux Services Web de l’ETNIC. Vous pouvez utiliser le certificat de votre carte d’identité (l’enregistrement se fait alors via les

écrans) ou bien un certificat acquis auprès d'un organisme de certification reconnu tel que GlobalSign ou Certipost. Dans ce dernier cas, vous devrez le communiquer par une autre voie à définir avec l'ETNIC.

2. COMMUNICATION ASYNCHRONE

2.1. ARCHITECTURE

La communication avec la plateforme Services Web de l'ETNIC se fait de manière asynchrone. C'est-à-dire que les réponses aux requêtes envoyées par le client sont récupérées de manière différées sur un service « Polling ». Ce dernier fournit les réponses dans l'ordre des requêtes reçues.
Ci-dessous est illustrée l'architecture globale de la plateforme en prenant comme exemple le service « SIEL – Inscription ». Le cheminement des messages y est décrit.



1. Le client envoie une requête fonctionnelle
2. L'ETNIC stocke sa demande pour traitement ultérieur
3. L'ETNIC lui renvoie un ID de corrélation disponible à 2 endroits dans le message SOAP de retour. L'application cliente doit stocker cet ID :
   - `/soap:Envelope/soap:Body/ow:StatutMsg/ow:message/ow:ID`
   - `/soap:Envelope/soap:Header/wsa:MessageID`
4. Lorsque le back-end du service SIEL est disponible, il traite la demande
5. La réponse est stockée dans une DB côté ETNIC

6. Le client envoie une requête de polling au service dédié

7. L'ETNIC lui renvoie une réponse fonctionnelle (ou une SOAP Fault) avec l'ID de corrélation disponible à 2 endroits dans le message :

    - `/soap:Envelope/soap:Body/poll:pollingReponse/poll:message/poll:ID`
    - `/soap:Envelope/soap:Header/wsa:RelatesTo`

    Le service « Polling » renvoie toujours la réponse la plus ancienne qui n'a pas encore été récupérée à destination du demandeur.

2.2. Routage des requetes

Comme l'URL d'accès est unique, quel que soir le service qui est appelé, la spécification **WS-Addressing** doit être utilisée pour adresser correctement le service demandé.

Il s'agit de remplir différentes informations dans la partie « Header » de l'enveloppe SOAP :

- Un champ **`wsa:To`** qui permet d'indiquer le service cible que l'on désire appeler
- Un champ **`wsa:Action`** qui définit la fonctionnalité que l'on désire appeler. L'ETNIC a adopté le standard suivant pour définir les actions:

  ```
  domaine:fonctionnalité?mode=sync/async
  ```

  Par exemple, pour le service « SIEL – Inscription », le domaine est « SIEL » et la fonctionnalité « inscription ». L'action pour l'adresser sera donc :

  ```
  siel:inscription?mode=async
  ```

  Les valeurs pour les champs `wsa:To` et `wsa:Action` à utiliser sont décrites dans les manuels d'utilisation spécifiques aux différents services, disponibles dans le catalogue de services SOA sur le site Internet de l'ETNIC.

- un champ **`wsa:From`** qui permet d'indiquer l'identité du demandeur afin de faire de l'audit, du traçage et des statistiques
- un champ **`wsa:MessageID`** qui permet de faire du traçage de message et de reconstituer un flux de messages (Attention dans le cas de la requête, il ne contient pas l'ID de corrélation décrit précédemment).

2.3. Service « Polling »

Le service « Polling » permet de récupérer les réponses fonctionnelles aux requêtes de manière différée. Pour l'invoquer, les valeurs spécifiques des champs WS-Addressing sont les suivantes :

- **wsa:To :** http://www.etnic.be/janus/polling
- **wsa:Action :** janus:polling?mode=sync

L’unique opération est `getMessage` et ne prend pas d’argument. La réponse renvoyée correspond à la plus vieille requête de l’appelant pour laquelle la réponse n’avait pas encore été récupérée, à l’instar d’une file FIFO *(first in first out).* La réponse contient le champ l’ID de corrélation par rapport à sa requête dans le champ **wsa:RelatesTo** présent dans l’entête du message. L’application appelante doit donc faire correspondre cet ID avec les IDs qu’elle a stockés de son coté pour faire correspondre la réponse avec la bonne requête (voir schéma d’architecture au point 2.1).

Le contrat WSDL du service « Polling » se trouve en téléchargement sur la page dédiée du service dans le catalogue de services SOA de l’ETNIC.

2.4. Exemple de messages de communication asynchrone

Les en-têtes relatifs à la sécurité ont été omis de l’exemple pour des raisons de lisibilité.

Requête fonctionelle :

```
<soapenv:Envelope xmlns:siel="http://www.etnic.be/janus/siel"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
 <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <wsa:Action>janus:fase?mode=async</wsa:Action>
  <wsa:From>
   <wsa:Address>http://etnic.be/soapui</wsa:Address>
  </wsa:From>
  <wsa:MessageID>uuid:81788842-deaf-4470-be48-4bd2e5ad453c</wsa:MessageID>
  <wsa:To>http://www.etnic.be/janus/fase</wsa:To>
 </soapenv:Header>
 <soapenv:Body>
  <ns1:FaseRequete xmlns:ns1="http://www.etnic.be/janus/fase">
   <ns1:Organisation>
    <ns1:Type>PO</ns1:Type>
    <ns1:Identifiant>763</ns1:Identifiant>
   </ns1:Organisation>
   <ns1:Dmd>FICHE</ns1:Dmd>
  </ns1:FaseRequete>
 </soapenv:Body>
</soapenv:Envelope>
```

Réponse contenant l’ID de correlation:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
 <soapenv:Header>

  <To>http://etnic.be/soapui</To>
  <MessageID>0000013d924e5d07-1247</MessageID>
  <RelatesTo>uuid:81788842-deaf-4470-be48-4bd2e5ad453c</RelatesTo>
  <From xmlns="http://www.w3.org/2005/08/addressing" >
   <Address>http://www.etnic.be/janus/fase</Address>
  </From>
  <wsa:Action soapenv:mustUnderstand="1"
   xmlns:wsa="http://www.w3.org/2005/08/addressing">janus:fase?mode=async</wsa:Action>
 </soapenv:Header>
 <soapenv:Body>
  <StatutMsg xmlns="http://www.etnic.be/janus/ow">
   <message>
    <ID>0000013d924e5d07-1247</ID>
```

```
   </message>
  </StatutMsg>
 </soapenv:Body>
</soapenv:Envelope>
```

Requête de polling :

```
<soapenv:Envelope xmlns:fase="http://www.etnic.be/janus/fase"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
 <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">

  <wsa:Action>janus:polling?mode=sync</wsa:Action>
  <wsa:From>
   <wsa:Address>http://etnic.be/soapui</wsa:Address>
  </wsa:From>
  <wsa:MessageID>uuid:28158767-4bb7-4b06-b7fe-a6d0b35ae884</wsa:MessageID>
  <wsa:To>http://www.etnic.be/janus/polling</wsa:To>
 </soapenv:Header>
 <soapenv:Body>
  <GetMessage/>
 </soapenv:Body>
</soapenv:Envelope>
```

Réponse fonctionnelle:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soapenv12="http://www.w3.org/2003/05/soap-envelope"
xmlns:wsa="http://www.w3.org/2005/08/addressing">
 <soapenv:Header>

  <wsa:To>http://etnic.be/soapui</wsa:To>
  <wsa:MessageID>uuid:28158767-4bb7-4b06-b7fe-a6d0b35ae884</wsa:MessageID>
  <wsa:RelatesTo>00000145279160df-246</wsa:RelatesTo>
  <wsa:From>
   <wsa:Address>http://www.etnic.be/janus/polling</wsa:Address>
  </wsa:From>
  <wsa:Action soapenv:mustUnderstand="1">janus:polling?mode=sync</wsa:Action>
 </soapenv:Header>
 <soapenv:Body>
  <pollingReponse xmlns="http://www.etnic.be/janus/polling"
xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
   <message>
    <ID>00000145279160df-246</ID>
    <Suivants>0</Suivants>
    <Contenu>
     <dedale:DedaleResponse xmlns:dedale="http://www.cfwb.be/dedale"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
      <dedale:Adresses>
       <dedale:Adresse>
        <dedale:Rue>Ruelle de Reuchamp</dedale:Rue>
        <dedale:Numero/>
        <dedale:BtePostale/>
        <dedale:CodePostal>1340</dedale:CodePostal>
        <dedale:Localite>OTTIGNIES-LOUVAIN-LA-NEUVE</dedale:Localite>
       </dedale:Adresse>
      </dedale:Adresses>
     </dedale:DedaleResponse>
    </Contenu>
   </message>
  </pollingReponse>
 </soapenv:Body>
</soapenv:Envelope>
```

3. SECURITE

3.1. Connexion securisee TLS

Les messages transitent à travers un canal HTTPS supportant le protocole TLS 1.0. Le chiffrement supporté est : ECDHE-RSA-AES256-SH
Les certificats de l'ETNIC pour les environnements TQ et PROD sont disponibles dans un fichier zip dans le catalogue de services SOA du site Internet de l'ETNIC.

3.2. Securisation des messages SOAP

Les messages SOAP transités sont sécurisés (signés) selon la spécification WS-Security en conjonction avec soit :

- Un certificat obtenu auprès d'un organisme de certification reconnu tel que GlobalSign ou Certipost. Dans ce cas la spécification WSS-x509TokenProfile de WS-Security est utilisée.
- Le certificat de la carte d'identité électronique de l'utilisateur. Dans ce cas-ci, ce certificat n'est pas utilisé directement pour signer les messages mais est utilisé pour obtenir un token de contexte de sécurité. C'est ce dernier qui est utilisé pour signer. Ce mécanisme est basé sur les spécifications WS-SecureConversation et WS-Trust.

3.2.1. WSS-x509TokenProfile

La spécification WSS-x509TokenProfile prévoit plusieurs possibilités pour référencer le certificat utilisé pour la signature. La méthode supportée par l'ETNIC consiste à référencer l'Issuer et le Serial Number.

Seul l'élément « Body » de l'enveloppe SOAP doit être signé.

Exemple d'un message signé par un certificat X509 :

```
<soapenv:Envelope xmlns:siel="http://www.etnic.be/janus/siel"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
 <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <wsse:Security soapenv:mustUnderstand="1" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
   <ds:Signature Id="SIG-752" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
      <ec:InclusiveNamespaces PrefixList="wsa siel soapenv"
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     </ds:CanonicalizationMethod>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
     <ds:Reference URI="#id-751">
      <ds:Transforms>
       <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
        <ec:InclusiveNamespaces PrefixList="siel" xmlns:ec="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
       </ds:Transform>
      </ds:Transforms>
```

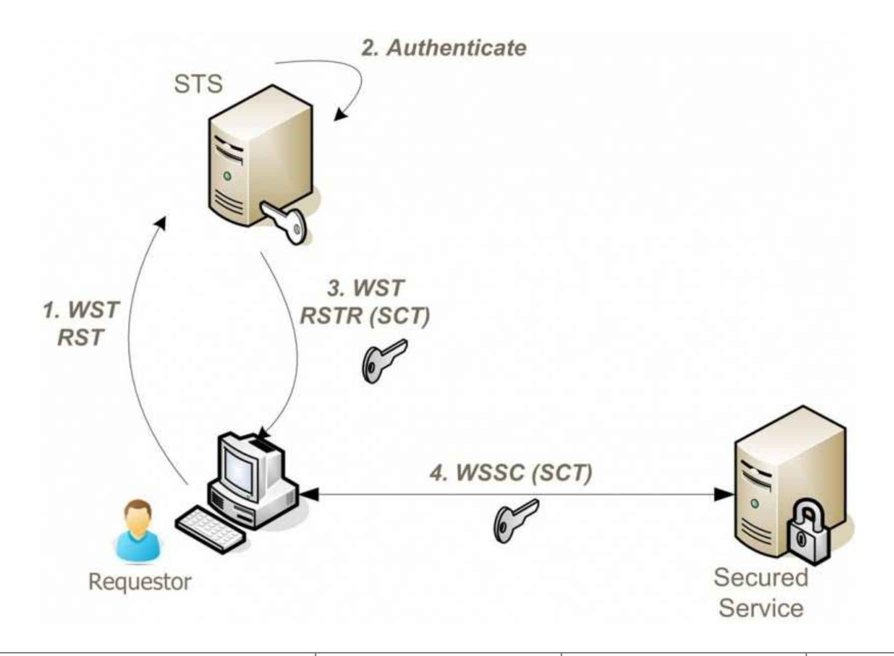
```
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>xC53nZkcNvpFd8vtucnvUwKPbsA=</ds:DigestValue>
     </ds:Reference>
    </ds:SignedInfo>

<ds:SignatureValue>hzm9/is5O7I5o3EZkVJ2jnbZiRSFSbFBl0YlW45mBqV2+8YRfHC1LVqafX7YLdVXTXrd1mWot1e
9+v31AiP3m5iy2+OCw7YhbxvCCCC0pbbfl/bpaeE/FE2f0sm4NZWsArpzlSEmd7DzpaiGxoMPWGxc
sefTSWHiC1u0RHy4HGERFBrHFDqDd2DMZHiugR0VxPz5QAacKeBnn68fZTK032Il+eOkyPaceuYH
YEbUEDjAFfhr1chc0wKzfZuxt0dn6pBdhlU499nX2xZ4dGE37fHAOvbNRZLg/U5/b+Knkkx/jEOe
9QJRSs/CKAONMfFcuZJnpZ+lbJoXT9UIKljdUA==</ds:SignatureValue>
    <ds:KeyInfo Id="KI-EAF95CB2EABEB3293D13643957589981127">
     <wsse:SecurityTokenReference wsu:Id="STR-EAF95CB2EABEB3293D13643957589981128">
      <ds:X509Data>
       <ds:X509IssuerSerial>
        <ds:X509IssuerName>CN=WSJanusTEST_BULL001</ds:X509IssuerName>
        <ds:X509SerialNumber>1243600900</ds:X509SerialNumber>
       </ds:X509IssuerSerial>
      </ds:X509Data>
     </wsse:SecurityTokenReference>
    </ds:KeyInfo>
   </ds:Signature>
  </wsse:Security>
 </soapenv:Header>
 <soapenv:Body wsu:Id="id-751" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-utility-1.0.xsd">  ...
 </soapenv:Body>
</soapenv:Envelope>
```

3.2.2. WS-Secure Conversation Token

Dans le cadre de l'utilisation du certificat de la carte d'identité électronique belge, il n'est pas envisageable de signer avec celui-ci car il impose de demander son code PIN à l'utilisateur pour chaque requête à signer avant envoi. C’est pourquoi un système de Security Token Service (STS) a été mis en place. Celui-ci peut être appelé via le standard WS-Trust afin de récupérer un jeton (token). C'est ce jeton qui servira à signer les requêtes suivantes jusqu'à son expiration.

Voici le schéma de ce principe :



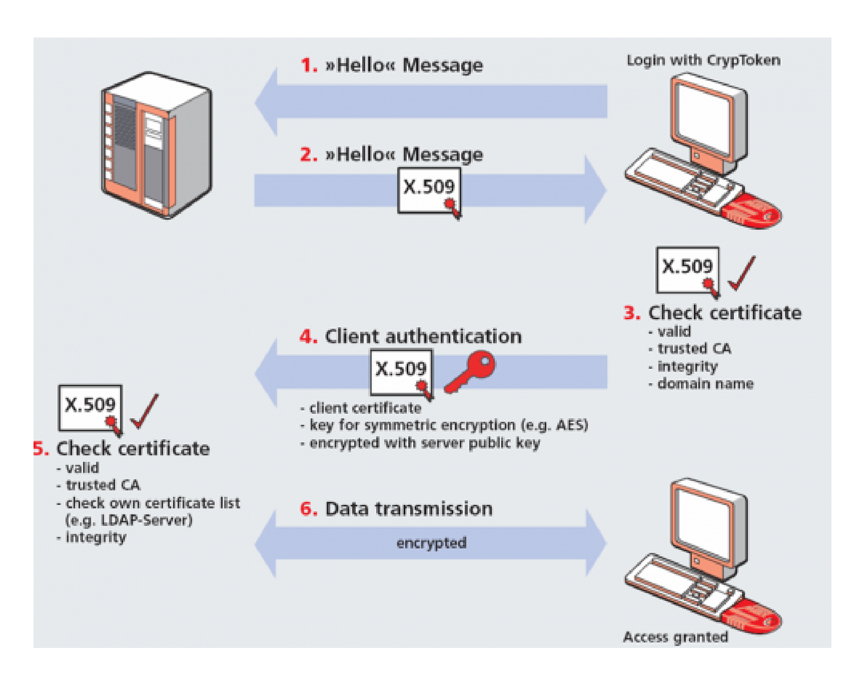
1. ***WST RST*** *(WS-Trust Request Security Token)* : Le client envoie une requête de demande de token au serveur STS.

   Exemple de requête :

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
 <soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd" wsu:Id="Id-18871350">
  <wst:RequestSecurityToken xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust">
   <wst:RequestType>http://schemas.xmlsoap.org/ws/2005/02/trust/Issue</wst:RequestType>
   <wst:TokenType>http://schemas.xmlsoap.org/ws/2005/02/sc/sct</wst:TokenType>
  </wst:RequestSecurityToken>
 </soapenv:Body>
</soapenv:Envelope>
```

2. Authenticate

L'authentification auprès du STS se fait via Mutual SSL, dont le fonctionnement est décrit ci-dessous :



Le certificat de la carte d'identité (enregistré à l'ETNIC) est ici utilisé et validé par le serveur STS pour authentifier le demandeur avant de lui remettre un token.

3. ***WST RSTR (SCT)*** *(WS-Trust Request Security Token Response (Security Context Token)):* Le STS renvoie le token (X.509) qui servira à signer au client.

   Exemple de réponse :

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
 <soap:Header>
  <wsse:Security soap:actor="secure_span" soap:mustUnderstand="1"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
```



Bâtiment 'Le Zénith'
Boulevard du Roi Albert II, 37
1030 Bruxelles


```
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
   <wsu:Timestamp wsu:Id="id-2-d8b6db1a929f7c149819ec183c1548e1">
    <wsu:Created>2014-02-19T10:09:43.114746992Z</wsu:Created>
    <wsu:Expires>2014-02-19T10:14:43.114Z</wsu:Expires>
   </wsu:Timestamp>
   <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="id-0-
b6b68eb710c70f895b1d2541064060c5">MIIDCjCCAfKgAwIBAgIIQmDAvqVfoKgwDQYJKoZIhvcNAQEMBQAwIzEhMB8G
A1UEAxMYc2VydmljZXMtd2ViLnRxLmV0bmljLmJlMB4XDTEzMDMxOTEzNTUwN1oXDTIzMDMxNzEzNTUwN1owIzEhMB8GA1
UEAxMYc2VydmljZXMtd2ViLnRxLmV0bmljLmJlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAokScCKxupNt8
+6x2auAK0bAoty0wK5xWee9fPHoRJAuiwdauo+s0PMDcD2rcWDT5G2QNHvmk+gzzyEu6aMaxxKEZUhtwruM5PkqNXMH+dH
X6JUKbgIgYlvvatA03GEU0UGnLr0V7u9cvmGzMU+aRMgUX8CtAsgmD0OurEiVcyW6rr84wX7os1Wx10VOHRL4edd6rT/AA
9ugoKLxc+wkR5CotUR5THkW3bhi6E+RkfVTlMk3KfOzt/i8mW5CdM+1caHq+W9igZKQGHChUDcu57fma+lJ4pb5EnaGOdI
VA3UvdaBo/Yz5Vr/d9GlsSgYsRtcI2Xj6YPJ0bTH/S+qpdXwIDAQABo0IwQDAdBgNVHQ4EFgQUaAiGpCdrMV+BIKCnmADi
T4rXuxMwHwYDVR0jBBgwFoAUaAiGpCdrMV+BIKCnmADiT4rXuxMwDQYJKoZIhvcNAQEMBQADggEBAJ+LE/2KqgACggYk3X
v0hd1Nmc0q9joEnIkE8PlcH7ZdWibwQwog9rf17yC90ExR5G2/kYPocy4iL+YED6x6i99AvhqNA8HTAjD0tCnMGEvJWPSk
B8huJdsuBLXnP1XDWzfXcyFj1JkGb8MEXpIOgmXDsv98bMYL6u+qFKehtUAhdZgPVqQVp4nClKJ6NGUHiXwjhZiWk2Hk2e
NgXX/CiG900cfLDUGpxkKN1hKaiOrYCmEMHxIPsxYf5R0D/YYAcZMOrO5QOy0JM/iW0boEUD0yErdrpPUeEb4VRiFx72TF
udDScJqNnwJCZn0cLcPkmJ/PHIWI/Bh+76tWLc1uUvs=</wsse:BinarySecurityToken>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
     <ds:Reference URI="#id-1-254d82d66e9957c180e856d1bf0109f6">
      <ds:Transforms>
       <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>D6F+imMesLRFAAjilmq3vYoJouA=</ds:DigestValue>
     </ds:Reference>
     <ds:Reference URI="#id-2-d8b6db1a929f7c149819ec183c1548e1">
      <ds:Transforms>
       <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>gw+8vQiLAmKyo10z1ShX1arhPRE=</ds:DigestValue>
     </ds:Reference>
    </ds:SignedInfo>

<ds:SignatureValue>b1qcN4cWaPd7mPDnFUUXTbZgFoXEREj6Fja8QVOPPSh1DZtKQf59IVljczMvZH3Jdglv6bWEWd0
KuBtsSniZQ4FyS4Qjx49oOGUl4AOr5y0kKRoGyiDZRxMjaQzH+mYOJjH55c9ZbtHtg2pIKxkuXHxjoS31RL6Y6s/l2SB2q
/rNlWVD2eJSVWok5DSSoCmPRAqTYe8Jq83BcgAMMPbLFICoibmcmiCsn3kpUWMmGQcElaE89QCRWrRGXLD95r/nE4ujNBb
dHt7h1bcSMxiu8EFEmgt4DdvFB6IF6vKf7jMIls+4qPCI5Z3lYHs2MxrNw5HnkM/dj+7puFXZh8C6sQ==</ds:Signatur
eValue>
    <ds:KeyInfo>
     <wsse:SecurityTokenReference xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
      <wsse:Reference URI="#id-0-b6b68eb710c70f895b1d2541064060c5"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3"/>
     </wsse:SecurityTokenReference>
    </ds:KeyInfo>
   </ds:Signature>
  </wsse:Security>
 </soap:Header>
 <soap:Body wsu:Id="id-1-254d82d66e9957c180e856d1bf0109f6" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <wst:RequestSecurityTokenResponse xmlns:wsc="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
   <wst:RequestedSecurityToken>
    <wsc:SecurityContextToken>

<wsc:Identifier>http://www.layer7tech.com/uuid/5d49793febfbbec46c5644fa0b05702f2be8cc9b</wsc:I
dentifier>
```

```
    </wsc:SecurityContextToken>
   </wst:RequestedSecurityToken>
   <wst:RequestedProofToken>
    <wst:BinarySecret
Type="http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey">gBndC3Zqhu6NiDBtM849Y7F4b89PnD
302MKwQ9tYXZI=</wst:BinarySecret>
   </wst:RequestedProofToken>
   <wst:Lifetime>
    <wsu:Expires>2014-02-19T12:09:43.113Z</wsu:Expires>
   </wst:Lifetime>
  </wst:RequestSecurityTokenResponse>
 </soap:Body>
</soap:Envelope>
```

4. ***WSSC (SCT)*** *(Ws-SecureConversation (Security Context Token)):* Les échanges avec le service sont maintenant sécurisés car signés par le token X.509 obtenu du serveur STS.

   Exemple de requête envoyée avec le SCT :

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
xmlns:wsa="http://www.w3.org/2005/08/addressing">
 <soapenv:Header>
  <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="true">
   <wsc:SecurityContextToken xmlns:wsc="http://schemas.xmlsoap.org/ws/2005/02/sc">

<wsc:Identifier>http://www.layer7tech.com/uuid/5d49793febfbbec46c5644fa0b05702f2be8cc9b</wsc:I
dentifier>
   </wsc:SecurityContextToken>
   <wsc:DerivedKeyToken xmlns:wsc="http://schemas.xmlsoap.org/ws/2005/02/sc"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="derivedKeyId-1">
    <wsse:SecurityTokenReference xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
     <wsse:Reference
URI="http://www.layer7tech.com/uuid/5d49793febfbbec46c5644fa0b05702f2be8cc9b"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd"/>
    </wsse:SecurityTokenReference>
    <wsc:Offset>0</wsc:Offset>
    <wsc:Length>20</wsc:Length>
    <wsc:Nonce>avVNfpeBDmnPscPZ9Mu6ww==</wsc:Nonce>
   </wsc:DerivedKeyToken>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-2">
    <ds:SignedInfo>
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
     <ds:Reference URI="#id-3">
      <ds:Transforms>
       <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>6w9ZxQHZRgU2IeZs1YRb0lNZTAM=</ds:DigestValue>
     </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>PAAK5JUh2kt+dPs/pgwmYYezogg=</ds:SignatureValue>
    <ds:KeyInfo Id="KeyId-3DF323081E1D4D392B13928045869761">
     <wsse:SecurityTokenReference xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="STRId-3DF323081E1D4D392B13928045869762"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
      <wsse:Reference URI="#derivedKeyId-1" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"/>
     </wsse:SecurityTokenReference>
```

```
    </ds:KeyInfo>
   </ds:Signature>
  </wsse:Security>
  ...
 </soapenv:Header>
 <soapenv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="id-3">
  ...
 </soapenv:Body>
</soapenv:Envelope>
```